

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-037589

(43)Date of publication of application : 07.02.2003

(51)Int.Cl.

H04L 9/14
G11B 20/10
H04L 9/08
// H04N 5/91

(21)Application number : 2001-226242

(71)Applicant : SONY CORP

(22)Date of filing : 26.07.2001

(72)Inventor : SAKO YOICHIRO

INOUCHI TATSUYA

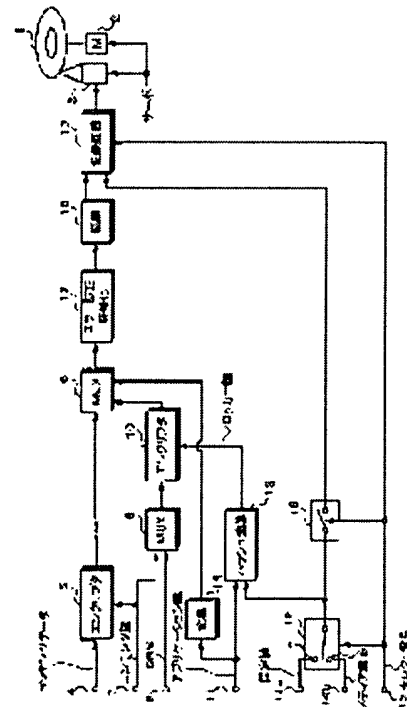
FURUKAWA SHUNSUKE

(54) DEVICE AND METHOD FOR DATA RECORDING, AND DEVICE AND METHOD FOR DATA REPRODUCING

(57)Abstract:

PROBLEM TO BE SOLVED: To easily introduce a new security system by using a fixed value instead of a key bound to the media and enciphering.

SOLUTION: An encryptor 5 enciphers a contents data which should be recorded by using a contents key. A locker key enciphers the contents key and DRM in encryptor 10. A hash value (the locker key) with an application key and the data chosen in a selector 12 (the fixed value or a media key) is calculated. The application key is data converted like scrambling in a conversion unit 14. The contents data enciphered, the contents key and DRM enciphered, and the application key converted are supplied to a record circuit 19 through an error correction coding device 17 and a modulation part 18, further, are recorded on an optical disk 1 with an optical pickup 3 together with the media key and a selection signal.



LEGAL STATUS

THIS PAGE BLANK (USPTO)

[Date of request for examination] 04.03.2003
[Date of sending the examiner's decision of rejection] 24.05.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(11)特許出願公開番号

特開2003-37589

(P2003-37589A)

(43)公開日 平成15年2月7日(2003.2.7)

(51) Int.Cl.⁷

識別記号

FI

テーマコード* (参考)

H04L 9/14

G 1 1 B 20/10

D 5 C 0 5 3

G 1 1 B 20/10

H 5D044

3 1 1 5 J 1 0 4

3 1 1

3 2 1 Z

3 2 1

H04L 9/00

641

審査請求 未請求 請求項の数22 OL (全 9 頁) 最終頁に続く

(21)出願番号

特願2001-226242(P2001-226242)

(22) 出願日

平成13年7月26日(2001.7.26)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 佐古 曜一郎

東京都品川区北品川6丁目7番35号 ソニ
一株式会社内

(72) 發明者 猪口 達也

東京都品川区北品川6丁目7番35号 ソニ
株式会社内

(74) 代理人 100082762

井理士 杉浦 正知

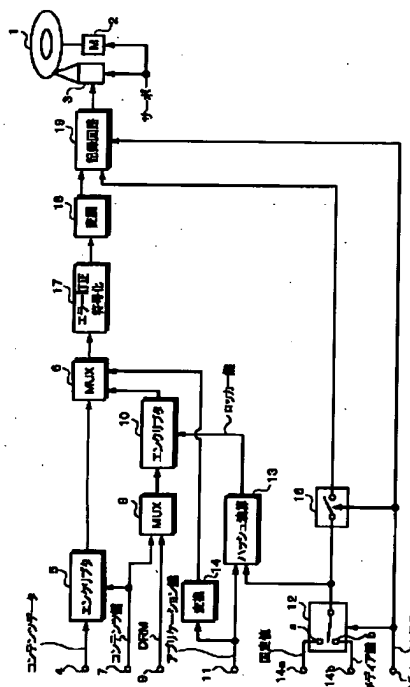
最終頁に続く

(54) 【発明の名称】 データ記録装置および方法、並びにデータ再生装置および方法

(57) 【要約】

【課題】メディアにバインドした鍵の代わりに固定値を使用して暗号化を行うことによって、新たなセキュリティシステムの導入を容易とする。

【解決手段】 記録すべきコンテンツデータがコンテンツ鍵を使用してエンクリプタ５によって暗号化される。コンテンツ鍵とDRMがエンクリプタ１０においてロッカー鍵によって暗号化される。アプリケーション鍵とセクタ１２で選択されたデータ（固定値またはメディア鍵）とのハッシュ値（ロッカー鍵）が演算される。アプリケーション鍵は、変換部１４において例えばスクランブルのようなデータ変換処理を受ける。暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵およびDRM、並びに変換されたアプリケーション鍵がエラー訂正符号化器１７および変調部１８を介して記録回路１９に供給され、メディア鍵とセレクト信号と共に、光ピックアップ３によって光ディスク１に記録される。



【特許請求の範囲】

【請求項 1】 コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、
上記コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録装置。

【請求項 2】 請求項 1 において、
上記コンテンツデータを媒体にバインドさせる場合には、上記媒体にバインドした鍵を使用して暗号化を行うようにしたデータ記録装置。

【請求項 3】 請求項 1 において、
上記固定値は、媒体の所定の領域に記録されるデータであるデータ記録装置。

【請求項 4】 請求項 1 において、
上記媒体にバインドした鍵は、媒体から読取可能であって、外部に出力されない識別情報であるデータ記録装置。

【請求項 5】 請求項 1 において、
上記媒体にバインドさせるか否かを識別するための識別情報を媒体に記録するデータ記録装置。

【請求項 6】 コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、
上記コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録方法。

【請求項 7】 請求項 6 において、
上記コンテンツデータを媒体にバインドさせる場合には、上記媒体にバインドした鍵を使用して暗号化を行うようにしたデータ記録方法。

【請求項 8】 請求項 6 において、
上記固定値は、媒体の所定の領域に記録されるデータであるデータ記録方法。

【請求項 9】 請求項 6 において、
上記媒体にバインドした鍵は、媒体から読取可能であって、外部に出力されない識別情報であるデータ記録方法。

【請求項 10】 請求項 6 において、
上記媒体にバインドさせるか否かを識別するための識別情報を媒体に記録するデータ記録方法。

【請求項 11】 コンテンツデータを暗号化して媒体に記録するデータ記録装置であって、
上記コンテンツデータを媒体にバインドさせる場合には、媒体にバインドした鍵を使用して暗号化を行い、
上記コンテンツデータを媒体にバインドさせない場合は、上記媒体にバインドした鍵に代えて固定値を使用して暗号化を行い、
上記固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録装置。

【請求項 12】 請求項 11 において、
上記再生環境を制限するための情報は、装置またはソフト

ウェアの識別子であるデータ記録装置。

【請求項 13】 コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、
上記コンテンツデータを媒体にバインドさせる場合には、媒体にバインドした鍵を使用して暗号化を行い、
上記コンテンツデータを媒体にバインドさせない場合は、上記媒体にバインドした鍵に代えて固定値を使用して暗号化を行い、
上記固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録方法。

【請求項 14】 請求項 13 において、
上記再生環境を制限するための情報は、装置またはソフトウェアの識別子であるデータ記録方法。

【請求項 15】 暗号化されたコンテンツデータを媒体から再生する再生装置であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記暗号化に使用する鍵を切り換えることによって、上記コンテンツデータを再生するデータ再生装置。

【請求項 16】 請求項 15 において、
上記暗号化が上記媒体にバインドされていない場合では、上記暗号化に使用する鍵として固定値を使用するデータ再生装置。

【請求項 17】 請求項 15 において、
上記暗号化が上記媒体にバインドされている場合では、上記復号方法に上記媒体にバインドしている鍵を使用するデータ再生装置。

【請求項 18】 暗号化されたコンテンツデータを媒体から再生する再生方法であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記復号に使用する鍵を切り換えることによって、上記コンテンツデータを再生するデータ再生方法。

【請求項 19】 請求項 18 において、
上記暗号化が上記媒体にバインドされていない場合では、上記復号に使用する鍵として固定値を使用するデータ再生方法。

【請求項 20】 請求項 18 において、
上記暗号化が上記媒体にバインドされている場合では、上記復号に上記媒体にバインドしている鍵を使用するデータ再生方法。

【請求項 21】 暗号化されたコンテンツデータを媒体から再生する再生装置であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記暗号化に使用する鍵を切り換えることによって、上記コンテンツデータを再生し、
上記暗号化が上記媒体にバインドする場合には、再生環境を制限せず、上記暗号化が上記媒体にバインドしない場合では、再生環境を制限するデータ再生装置。

【請求項22】 暗号化されたコンテンツデータを媒体から再生する再生方法であって、
上記暗号化を復号する際に、上記暗号化が上記媒体にバインドされているか否かを判別し、判別結果に応じて上記暗号化に使用する鍵を切り換えることによって、上記コンテンツデータを再生し、
上記暗号化が上記媒体にバインドする場合には、再生環境を制限せず、上記暗号化が上記媒体にバインドしない場合では、再生環境を制限するデータ再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化によってセキュリティを保つようにしたデータ記録装置および方法、並びにデータ再生装置および方法に関する。

【0002】

【従来の技術】近年、音楽情報が記録されたCD (Compact Disc)のデジタルデータをMP3で圧縮したコンテンツがインターネットを介して配信されたり、CD-R (CD-Recordable)を使用してCDがコピーされたり、米Napster社が提供するピア・ツー・ピア型の音楽ファイルの交換サービスが広まっており、著作権保護（以下、適宜セキュリティと称する）の問題が大きくクローズアップされている。このため、近年提案されている新規なメディア（SACD (Super Audio CD)、DVD (Digital Versatile Disc またはDigital Video Disc) オーディオ、メモ리카ード、データプレイディスク等）では、コンテンツを暗号化し、セキュリティを保っている。例えばメモ리카ードは、フラッシュメモリを使用し、機器に着脱自在とされたもので、暗号化された音楽データをメモ리카ードに記録しようとする、認証が行なわれ、認証が成立して初めて暗号化データを記録することが可能となる。

【0003】また、データプレイディスクは、米DataPlay社の提案による小型光ディスク（直径3.2mm）であり、著作権保護技術が採用されている。この技術は、暗号化とコンテンツの再生条件を制御する技術で構成される。著作権保護システムのみがアクセスできるディスク内周部の専用領域にコンテンツの暗号を解く「暗号化キー」とユーザによるアクセス条件を規定する「条件アクセスキー」が格納される。

【0004】また、鍵情報そのものではなく、鍵情報を生成するのに不可欠な情報を再生専用領域（ROM部分）に記録することが考えられている。例えばDVDの不正コピー防止技術として、書き換え可能なDVDの最内周部の再生専用領域（ROM部分）にメディアIDを記録し、メディアIDとMKB (Media Key Block) のハッシュ値を鍵データとして暗号化されたコンテンツをそのディスクに記録することが提案されている。メディアIDは、ディスク毎に異なる値であり、ユーザが書き換えることができないので、たとえデータ部分を他の別の

ディスクに不正にコピーしても、メディアIDが元のディスクとは異なるので、そのデータ部分を復号することが不可能である。

【0005】

【発明が解決しようとする課題】上述したような著作権保護対策がなされた新規メディアを利用するためには、新規なレコーダ/プレーヤを購入する必要がある。このことは、ユーザに新たな負担を生じさせるので、新規メディアが広く普及する妨げとなる。一方、既存のレコーダ/プレーヤに著作権保護対策を導入しようとしても、互換性の問題が生じたり、互換性をとるためにパーソナルコンピュータにインストールしたソフトウェアで暗号化を復号しようすると、十分な著作権保護ができない問題があった。

【0006】したがって、この発明の目的は、メディアにバインドした鍵を使用して暗号化する本格的なセキュリティ機能の導入を容易とすることが可能なデータ記録装置および方法、並びにデータ再生装置および方法を提供することにある。

【0007】

【課題を解決するための手段】上述した課題を達成するために、請求項1の発明は、コンテンツデータを暗号化して媒体に記録するデータ記録方法であって、コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録装置である。請求項6の発明は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行うようにしたデータ記録方法である。

【0008】請求項11の発明は、コンテンツデータを暗号化して媒体に記録するデータ記録装置であって、コンテンツデータを媒体にバインドさせる場合には、媒体にバインドした鍵を使用して暗号化を行い、コンテンツデータを媒体にバインドさせない場合は、媒体にバインドした鍵に代えて固定値を使用して暗号化を行い、固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録装置である。請求項13の発明は、固定値を使用して暗号化する場合では、再生環境を制限するための情報を記録するデータ記録方法である。

【0009】請求項15の発明は、暗号化されたコンテンツデータを媒体から再生する再生装置であって、暗号化を復号する際に、暗号化が媒体にバインドされているか否かを判別し、判別結果に応じて暗号化に使用する鍵を切り換えることによって、コンテンツデータを再生するデータ再生装置である。請求項18の発明は、判別結果に応じて復号に使用する鍵を切り換えることによって、コンテンツデータを再生するデータ再生方法である。

【0010】請求項21の発明は、暗号化されたコンテンツデータを媒体から再生する再生装置であって、暗号

化を復号する際に、暗号化が媒体にバインドされているか否かを判別し、判別結果に応じて暗号化に使用する鍵を切り換えることによって、コンテンツデータを再生し、暗号化が媒体にバインドする場合には、再生環境を制限せず、暗号化が媒体にバインドしない場合では、再生環境を制限するデータ再生装置である。請求項22の発明は、暗号化が媒体にバインドしない場合では、再生環境を制限するデータ再生方法である。

【0011】この発明では、媒体にバインドしていないが、媒体にバインドした鍵と同様に暗号化の鍵として機能する固定値を使用することを可能とする。固定値を使用して暗号化されたコンテンツデータの記録された媒体は、媒体にバインドした鍵で暗号化されたコンテンツデータの記録された媒体と殆ど同一のセキュリティシステムで扱うことが可能となり、互換性を容易にとることができる。この発明は、媒体にバインドした鍵を使用する本格的セキュリティシステムの導入を容易とすることができる。

【0012】

【発明の実施の形態】以下、この発明の一実施形態について説明する。この一実施形態は、光ディスクに対してこの発明を適用した例である。図1を参照して、記録装置の一例について説明する。図1において、参照符号1が光ディスク例えばCD-RWまたはCD-Rと同様の記録可能な光ディスクを示す。この光ディスク1に対して記録されるコンテンツデータは、全て暗号化されるものと規定されている。したがって、暗号化を行なわない既存のドライブによって、光ディスク1を使用して記録および再生を行うことができない。

【0013】図1に示す記録装置および後述する再生装置(図2)は、専用のハードウェアに限らず、パーソナルコンピュータとソフトウェアによって実現することが可能である。特に、セキュリティに関連する暗号化および復号化の処理をソフトウェアによって実現するようになされる。

【0014】光ディスク1は、スピンドルモータ2によって、線速度一定または角速度一定で回転駆動される。光ディスク1にデータを記録し、光ディスク1に記録されたデータを読み出すために、光ピックアップ3が設けられている。光ピックアップ3が送りモータ(図示しない)によって光ディスク1の径方向に送られる。

【0015】この一実施形態の光ディスク1は、記録に必要なとされる出力レベルのレーザ光を照射することによってデータの記録が可能で、光ディスク1によって反射されたレーザ光の光量の変化を検出することによって再生可能な相変化型ディスクである。相変化記録材料からなる記録膜が被着される基板の材質は、例えばポリカーボネートであり、ポリカーボネートを射出成形することによって、基板上にグループと呼ばれるトラック案内溝が予め形成されている。このディスク基板上に形成され

るグループは、予め形成する意味でプリグループとも呼ばれ、グループの間は、ランドと呼ばれる。通常、読取レーザ光の入射側から見て手前側がランドであり、遠い側がグループであると定義される。グループは、内周から外周へスパイラル状に連続して形成されている。なお、この発明は、記録可能であれば、相変化型光ディスクに限らず、光磁気ディスク、有機色素を記録材料として使用する追記形ディスクに対しても適用できる。

【0016】グループは、光ディスク1の回転制御用と記録時の基準信号とするために光ディスクの径方向に蛇行(ウォブルと称する)している。データは、グループ内、またはグループおよびランドに記録される。さらに、グループのウォブル情報としてアドレス情報としての絶対時間情報を連続的に記録している。CD-Rディスク、CD-RWディスクでは、グループのウォブル情報によって得られるアドレス情報としての絶対時間情報を参照して光ディスク1上の所望の書き込み位置を検索し、光ピックアップ3を移動させ、光ピックアップ3から光ディスク1に対してレーザ光を照射することによって、データをディスクに書き込むようにしている。

【0017】このようなウォブリングしたグループを有する光ディスクは、以下のようにして製造される。マスタリング装置は、ディスク状のガラス原盤に塗布されたフォトレジスト膜にレーザ光を照射すると共に、レーザ光を径方向に偏向または径方向に振ることによって、アドレス情報、クロック情報等を有するウォブリンググループを形成する。レーザ光の照射によって露光されたフォトレジスト膜を現像することによってディスク原盤が作成され、ディスク原盤から電鍍処理によってスタンプが作成され、スタンプを用いて射出成形を行うことによって、上述したウォブルグループを有するディスク基板が成形される。このディスク基板に相変化型の記録材料をスパッタリング等の手法を用いて被着することによって光ディスクが作成される。

【0018】図1に戻ると、記録すべきコンテンツデータ例えばオーディオおよび/またはビデオデータが入力端子4からエンクリプタ5に供給される。エンクリプタ5によって暗号化されたコンテンツデータがマルチプレクサ6に供給される。エンクリプタ5は、入力端子7からのコンテンツ鍵を使用してコンテンツデータに対して暗号化を施す。コンテンツ鍵は、マルチプレクサ8に対しても供給される。

【0019】マルチプレクサ8に対してどのようにコンテンツを扱うかを指示する管理情報(DRM(Digital Rights Management)と表記する)が入力端子9から供給される。例えばコピーの可否、コピー世代の管理の情報がDRMに含まれている。マルチプレクサ8の出力データがエンクリプタ10によって暗号化される。このエンクリプタ10は、コンテンツ鍵とDRMとを暗号化するためのものである。エンクリプタ10から出力される暗

10

20

30

40

50

号化されたコンテンツ鍵およびDRMがマルチプレクサ6に対して供給される。

【0020】エンクリプタ10に対しては、ロッカー鍵が供給され、ロッカー鍵によってコンテンツ鍵およびDRMが暗号化される。ハッシュ演算部13において、入力端子11からのアプリケーション鍵とセクタ12で選択されたデータとのハッシュ値が演算される。このハッシュ値がロッカー鍵である。アプリケーション鍵は、メディアにバインドしていない鍵を意味し、ソフトウェアにより保持され、または、デバイスにより保持されている。アプリケーション鍵は、変換部14において例えばスクランブルのようなデータ変換処理を受け、マルチプレクサ6に供給される。

【0021】メディアにバインドしている鍵とは、そのメディアに記録されることによって、そのメディアに専用の鍵となるものを意味する。メディアにバインドしている鍵は、暗号化によるセキュリティ対策を行なわない既存のドライブによってメディアを再生した時には、読み取れないように、そのメディアに埋め込まれている。一方、セキュリティ対策を行う新規なドライブによつて、メディアにバインドしている鍵を読み取ることが可能とされている。具体的には、ビット自身の変形またはビットの変位（ウォブリング）により表される鍵、EFM変調における結合ビット（3ビット）を使用して表現された鍵、ディスク最内周領域に記録されたディスク固有のID等がメディアにバインドしている鍵である。新規なドライブは、メディアにバインドしている鍵を抽出し、抽出された鍵によって暗号化コンテンツを復号することができる。しかしながら、新規なドライブは、鍵自体を外から知ることができないような対策がとられているのが普通であり、暗号化コンテンツと鍵とを不正にコピーしたメディアを作成することが不可能とされている。

【0022】セクタ12は、第1の入力端子a、第2の入力端子bおよび出力端子を有し、入力端子aと接続された入力端子14aには、固定値が供給され、入力端子bと接続された入力端子14bには、メディア鍵が供給される。セクタ12は、例えばドライブ全体の動作を制御するソフトウェアに基づいて形成され、入力端子15に供給されるセレクト信号によって制御される。セクタ12が選択したメディア鍵および固定値の一方がハッシュ演算部13およびゲート16に供給される。

【0023】以下、固定値が選択されてデータが記録される光ディスク、すなわち、メディアにバインドしない光ディスクをタイプAのディスクと適宜呼び、メディア鍵が選択されてデータが記録される光ディスク、すなわち、メディアにバインドした光ディスクをタイプBのディスクと適宜呼ぶことにする。タイプAおよびタイプBの何れのディスクも、暗号化されたコンテンツデータが記録されるものである。

【0024】ドライブ全体の動作を制御するソフトウェアは、CD-ROM等のメディア、またはネットワークを介して配布されたものである。例えばメディア鍵が記録されたタイプBのディスクを再生できる新規ドライブが未だ十分に普及していない段階では、固定値を選択するようにセクタ12を制御するセレクト信号をソフトウェアが発生するようになされる。その後、新規ドライブが十分に普及した段階では、メディア鍵を選択するようにセクタ12を制御するセレクト信号を発生するソフトウェアが配布される。なお、ユーザが所有しているドライブがタイプAおよびタイプBの何れのディスクに対応しているかに応じてセレクト信号を発生しても良い。

【0025】固定値を使用して暗号化されたタイプAのディスクは、既存のプレーヤで再生することができない。しかしながら、固定値を使用して暗号化を復号するデクリプタを既存のプレーヤに付加する変更を加えれば、タイプAのディスクを再生することができる。メディア鍵の読取、ロッカー鍵およびコンテンツ鍵の生成等の処理に必要な構成を付加する必要がないので、比較的ローコストな構成が可能である。さらに、暗号化の復号をソフトウェア処理を行う場合では、タイプAの光ディスクを既存のドライブで再生し、固定値を使用して復号することができる。この場合では、ドライブ側に対してハードウェアの変更を殆ど行わずにタイプAのディスクを再生することが可能となる。

【0026】メディア鍵は、上述したメディア（ここでは光ディスク1）にバインドしている鍵を意味する。一方、固定値は、メディアにバインドしていない値である。例えば全て“1”のデータ、全て“0”のデータ、“101010・・・10”のような既知のパターンのデータが固定値である。さらに、光ディスク1の最内周側のリードイン領域の特定のアドレスに記録されている特定のデータを固定値として使用しても良い。例えばTOC(Table Of Contents)中のプログラムスタート時間、曲数のデータ、そのディスクの総演奏時間のデータ等を使用できる。メディア鍵は、光ディスク1に必ず記録されるが、ドライブシステムにとって既知の固定値は光ディスク1に記録する必要がない。上述したTOC中の所定のデータを固定値とする場合では、TOCデータ自身がドライブによって記録されるので、殊更、固定値を記録する必要はない。

【0027】メディア鍵を光ディスク1に記録するために、ゲート16は、セクタ12がメディア鍵を選択する時にオンするように、セレクト信号によって制御される。セクタ12が固定値を選択する時には、ゲート16がオフとされる。ゲート16の出力が記録回路19に供給される。

【0028】マルチプレクサ6は、暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵およびDRM、

10

20

30

40

50

並びに変換されたアプリケーション鍵を所定のデータフォーマットに変換する。マルチプレクサ6の出力データがエラー訂正符号化器17に供給される。エラー訂正符号化器17によってエラー訂正符号化の処理がなされる。エラー訂正符号化器17の出力が変調部18で変調される。例えばE FM変調の処理がなされる。変調部18の出力が記録回路19に供給される。

【0029】記録回路19に対してゲート16から出力されるメディア鍵とセクタ12を制御するセレクト信号とが供給される。記録回路19では、フレーム同期信号、アドレス等の付加の処理を行い、また、メディア鍵およびセレクト信号がそれぞれ記録データに変換される。例えばE FM変調における結合ビット(3ビット)を利用してメディア鍵が光ディスク1に対して記録される。この場合では、メディア鍵を変調部18に供給するようにしても良い。また、リードインエリアのTOCの一部のデータとしてセレクト信号に基づいて生成されたタイプ識別子が記録される。さらに、記録回路19のレーザドライブでは、光ディスク1に対して記録データを記録するための所定のレベルを有するドライブ信号が生成される。レーザドライブの出力が光ピックアップ3の半導体レーザに対して供給され、半導体レーザからドライブ信号に基づいて変調されたレーザ光が光ディスク1に照射され、データが記録される。

【0030】図2は、この発明が適用され、図1の記録系に対応する再生系の構成の一例を示す。光ディスク1に光ピックアップ3から再生に必要とされるレーザ光を照射し、光ピックアップ3に設けられた4分割フォトディテクタによって光ディスク1によって反射されたレーザ光を決定する。検出された信号がRF処理ブロック21に供給される。RF処理ブロック21では、マトリックスアンプがフォトディテクタの検出信号を演算することによって、再生(RF)信号、トラッキングエラー信号、フォーカスエラー信号を生成する。ウォプリンググループの情報としてクロックおよびアドレスが記録されている場合では、ウォブル信号がRF処理ブロック21から出力される。なお、記録系と同様に再生系も、専用のハードウェアに限らず、パーソナルコンピュータとソフトウェアによって実現することが可能である。

【0031】RF信号が復調部22に供給され、例えばE FM復調がなされる。復調部22の出力データがエラー訂正回路23に供給され、エラー訂正処理がなされる。エラー訂正回路23の出力信号がデマルチプレクサ24およびタイプID(識別子)読取部25に供給される。図示しないサーボ回路に対して、トラッキングエラー信号、フォーカスエラー信号が供給され、スピンドルモータ2の回転および光ピックアップ3のトラッキングおよびフォーカスが制御される。サーボ回路は、光ピックアップ3に対するトラッキングサーボおよびフォーカスサーボと、スピンドルモータ2に対するスピンドルサ

ーボと、スレッドサーボを行う。また、ウォブル信号を復調することによってアドレス情報が取り出される。このアドレス情報は、ATIP(Absolute Time In Pre-groove)と称され、時間情報によってディスク上の絶対アドレスを示すものである。アドレス情報は、システムコントローラ(図示しない)に供給され、光ディスク1上の所望のアドレスの情報を読み取るようになされる。

【0032】デマルチプレクサ24は、暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵およびDRM、並びに変換されたアプリケーション鍵を分離して出力する。暗号化されたコンテンツデータが暗号化の復号を行うデクリプタ26に供給される。デクリプタ26によって暗号化が復号され、出力端子27には、光ディスク1から再生され、復号されたコンテンツデータが取り出される。

【0033】デマルチプレクサ24で分離された暗号化されたコンテンツ鍵およびDRMがデクリプタ28に供給され、変換されたアプリケーション鍵が逆変換部29に供給される。逆変換部29は、記録系(図1参照)の変換部14でなされた変換処理と逆の処理を行なうものである。例えば記録系でアプリケーション鍵に対してスクランブル処理が施される場合では、逆変換部29では、デスクランブル処理がなされる。逆変換部29から出力されるアプリケーション鍵がハッシュ演算部30に供給される。

【0034】ハッシュ演算部30には、セクタ31の出力も供給されている。セクタ31の一方の入力端子aには、デマルチプレクサ24から出力される固定値が供給され、その他方の入力端子bには、RF処理ブロック21で分離されたメディア鍵が供給される。固定値は、例えばTOCの一部に記録されている特定のデータである。デマルチプレクサ24は、固定値を分離して出力する。デマルチプレクサ24が固定値を発生し、発生した固定値を出力するようにしても良い。

【0035】メディア鍵は、光ディスク1(タイプB)にバインドしている鍵であり、外部から知ることが殆ど不可能なように、秘密に光ディスク1に記録されている。光ディスク1がタイプAのディスクであれば、メディア鍵が記録されていない。セクタ31は、タイプID読取部25から出力されるタイプIDによって制御される。

【0036】タイプIDは、例えば光ディスク1の最内周部のTOCの一部のデータとして記録される。光ディスク1をドライブに装着した場合、最初にTOC領域の情報が読み出される。タイプIDがタイプAのディスクを示している場合では、入力端子aが選択され、デマルチプレクサ24からの固定値がハッシュ演算部30に供給される。タイプIDがタイプBのディスクを示している場合では、入力端子bが選択され、RF処理ブロック21からのメディア鍵がハッシュ演算部30に供給され

る。ハッシュ演算部 30 が二つの入力のハッシュ値を求める。求められたハッシュ値がロッカー鍵である。

【0037】ハッシュ演算部 30 からのロッカー鍵がデクリプタ 28 に供給される。デクリプタ 28 によって、コンテンツ鍵および DRM に対して施されている暗号化が復号される。デクリプタ 28 に接続されたデマルチプレクサ 32 は、コンテンツ鍵と、DRM とを分離して出力する。コンテンツ鍵が上述したデクリプタ 26 に供給され、コンテンツデータの暗号化が復号される。DRM が出力端子 33 に取り出される。

【0038】図 3 は、タイプ判別とセクタ 31 の制御動作の流れを示すフローチャートである。最初のステップ S1 において、タイプ ID の読取がなされる。読み取られたタイプ ID に基づいて、再生しようとする光ディスク 1 がタイプ A か否かがステップ S2 において判定される。タイプ A のディスクであると判定されると、デマルチプレクサ 24 からの固定値をセクタ 31 が選択的に出力する（ステップ S3）。図 3 の例では、全て "1" の 128 ビットのデータを固定値として使用する例が示されている。

【0039】タイプ A のディスクでないと、ステップ S2 で判定された場合は、ステップ S4 において、タイプ B のディスクであるか否かが判定される。タイプ B のディスクと決定されるならば、ステップ S5 においてメディア鍵の読取がなされる。そして、読み取られたメディア鍵がステップ S6 においてセクタ 31 から出力される。若し、ステップ S4 において、タイプ B のディスクでないと判定されると、タイプ A および B の何れでもないとの判定結果となる。この場合は、エラー処理がなされる（ステップ S7）。

【0040】上述したこの発明の一実施形態において、メディアにバインドしていない固定値を使用している場合は、全く同一のコピーメディアが作成可能となるので、著作権保護が不十分となる。この影響を軽減するために、固定値を使用したタイプ A のディスクの場合では、再生環境を制限することが好ましい。例えばタイプ A のディスクでは、コンテンツデータをその光ディスクに記録したソフトウェアまたはハードウェアの ID（識別子）をディスクに記録し、その ID を共有している装置のみがそのコンテンツデータを再生できるようになされる。極端な例は、記録を行なったドライブまたはソフトウェアのみがその光ディスクを再生することが可能とされる。一方、メディア鍵を使用している場合は、再生環境を制限しないようになされる。

【0041】この発明は、上述したこの発明の一実施形

態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば使用する光ディスクとして、タイプ A および B 以外の第 3 のタイプのものを使用しても良い。第 3 のタイプの光ディスクは、読み出し専用エリアにその光ディスク固有の識別情報が記録されたものである。そして、この識別情報を使用して求めたハッシュ値を鍵データとして暗号化がなされる。第 3 のタイプの光ディスクの記録および／または再生を可能とするようにしても良い。また、この発明は、書き換え可能形光ディスク、追記形光ディスク以外に読み出し専用形光ディスクに対しても適用することができる。読み出し専用形の場合では、図 1 に示す記録装置は、マスタリング装置に対して適用される。さらに、この発明は、光ディスク限らず、他のデータ記録媒体例えばメモ리카ードに対しても適用することができる。

【0042】

【発明の効果】この発明では、メディアにバインドしているメディア鍵を使用した本格的なセキュリティ機能を実現する新規なドライブが普及していない段階では、本格的なセキュリティ機能との互換性を有する、固定値を使用したセキュリティ機能を実現することによって、新規なドライブをスムーズに導入することが可能となる。また、メディアにバインドしているか否かをタイプ ID で識別することによって、メディア鍵を使用したセキュリティ機能と固定値を使用したセキュリティ機能とを同じセキュリティシステム上でハンドリングすることができ、互換性を容易にとることができる。さらに、メディアにバインドしていない固定値を使用した場合でも、再生環境を制限することによって、セキュリティを保持することができる。

【図面の簡単な説明】

【図 1】この発明の一実施形態における記録装置の構成例を示すブロック図である。

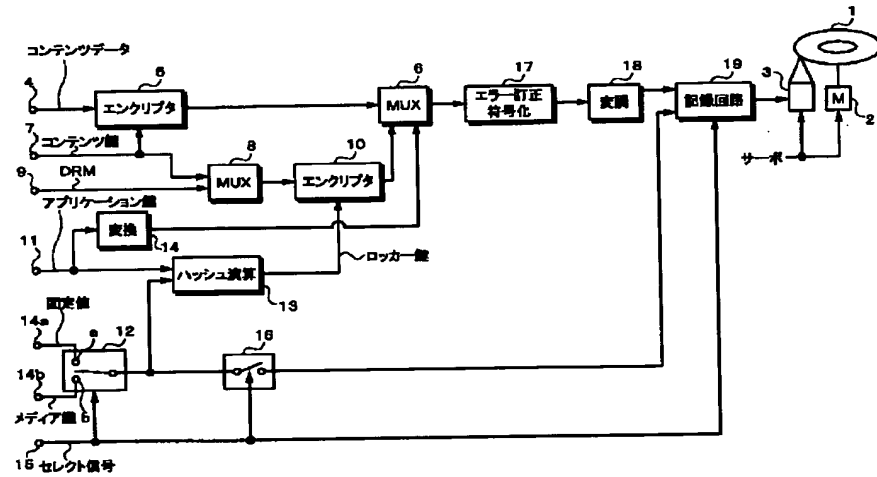
【図 2】この発明の一実施形態における再生装置の構成例を示すブロック図である。

【図 3】この発明の一実施形態におけるタイプ識別動作の処理の流れを示すフローチャートである。

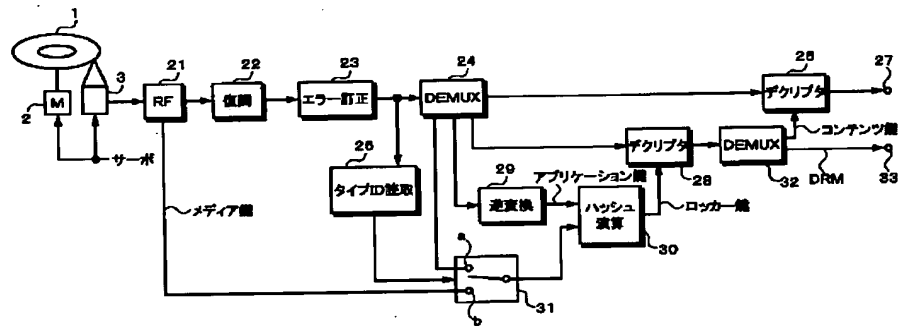
【符号の説明】

1・・・光ディスク、3・・・光ピックアップ、5、10・・・エンクリプタ、7・・・コンテンツ鍵の入力端子、12・・・セクタ、13・・・ハッシュ演算部、14a・・・固定値の入力端子、14b・・・メディア鍵の入力端子、15・・・セレクト信号の入力端子

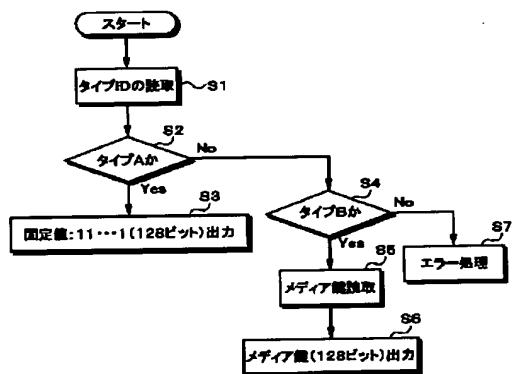
【図1】



【図2】



【図3】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テーマコード(参考)	
H 0 4 L	9/08	H 0 4 L	9/00	6 0 1 Z
// H 0 4 N	5/91	H 0 4 N	5/91	P

(72) 発明者 古川 俊介
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5C053 FA13 FA23 GB15 JA21 LA06
5D044 AB05 BC05 BC06 CC06 DE02
DE03 DE12 DE49 DE50 DE53
DE57 DE58 EF05 FG18 GK12
GK17
5J104 AA16 EA06 EA17 NA02 NA12
PA14

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第7部門第3区分
 【発行日】平成15年6月20日(2003. 6. 20)

【公開番号】特開2003-37589(P2003-37589A)
 【公開日】平成15年2月7日(2003. 2. 7)
 【年通号数】公開特許公報15-376
 【出願番号】特願2001-226242(P2001-226242)
 【国際特許分類第7版】

H04L 9/14

G11B 20/10

311

321

H04L 9/08

// H04N 5/91

【F I】

H04L 9/00 641

G11B 20/10 D
H

311

321 Z

H04L 9/00 601 Z

H04N 5/91 P

【手続補正書】

【提出日】平成15年3月4日(2003. 3. 4)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正内容】

【発明の名称】記録媒体の記録装置および方法、記録媒体の再生装置および方法、並びに記録媒体

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理を施す暗号化処理部と、

上記暗号化処理部からの出力データにエンコード処理を施すとともに、上記暗号化処理部で上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込むエンコード処理部と、上記エンコード処理部からの出力データを記録媒体に記

録する記録部とを備えている記録媒体の記録装置。

【請求項2】 上記暗号化処理部は、上記入力されたコンテンツデータにコンテンツ鍵データを用いて暗号化処理を施すエンクリプタを備えている請求項1に記載の記録媒体の記録装置。

【請求項3】 上記暗号化処理部は、更に上記コンテンツ鍵データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理を行う更なるエンクリプタを備えている請求項2に記載の記録媒体の記録装置。

【請求項4】 上記更なるエンクリプタは、上記コンテンツ鍵データとともに上記コンテンツデータの著作権管理データを暗号化処理する請求項3に記載の記録媒体の記録装置。

【請求項5】 上記暗号化処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データのいずれかのデータとアプリケーション鍵データとにより演算処理を行う演算処理部を備え、上記演算処理部からの出力データを上記更なるエンクリプタに暗号化処理のための鍵データとして供給する請求項3に記載の記録媒体の記録装置。

【請求項6】 上記エンクリプタからの出力データと上記アプリケーション鍵データと上記更なるエンクリプタからの出力データは、上記エンコード処理部に供給され

る請求項 4 に記載の記録媒体の記録装置。

【請求項 7】 上記暗号化処理部は、更に上記アプリケーション鍵データを変換する変換回路部を備え、上記変換回路部からの出力データが上記エンコーダに供給される請求項 6 に記載の記録媒体の記録装置。

【請求項 8】 上記装置は、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データを上記記録媒体に記録する請求項 1 に記載の記録媒体の記録装置。

【請求項 9】 入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、上記暗号化処理されたデータにエンコード処理を施す際に、上記暗号化処理の際に上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、上記エンコード処理されたデータを記録媒体に記録する記録媒体の記録方法。

【請求項 10】 上記方法は、上記入力されたコンテンツデータに先ずコンテンツ鍵データを用いて暗号化処理を施す請求項 9 に記載の記録媒体の記録方法。

【請求項 11】 上記方法は、更に上記コンテンツ鍵データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理を行う請求項 10 に記載の記録媒体の記録方法。

【請求項 12】 上記方法は、上記コンテンツ鍵データとともに上記コンテンツデータの著作権管理データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理する請求項 11 に記載の記録媒体の記録方法。

【請求項 13】 上記方法は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データのいずれかのデータとアプリケーション鍵データとにより演算処理を行い、上記演算処理の結果得られるデータを用いて上記コンテンツ鍵データを暗号化処理する請求項 11 に記載の記録媒体の記録方法。

【請求項 14】 上記方法は、上記暗号化されたコンテンツデータと上記アプリケーション鍵データと上記暗号化されたコンテンツ鍵データとがエンコード処理される請求項 13 に記載の記録媒体の記録方法。

【請求項 15】 上記方法は、上記アプリケーション鍵データは所定の変換処理が施されたあとにエンコード処理が施される請求項 14 に記載の記録媒体の記録方法。

【請求項 16】 上記方法は、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データを上記記録媒体に記録する請求項 9 に記載の記録媒体の記録方法。

【請求項 17】 コンテンツデータが暗号化されて記録されている記録媒体からデータを読み出すヘッド部と、上記ヘッド部からの信号にデコード処理を施すデコーダと、

上記記録媒体から読み出された上記記録媒体に記録されることによって記録媒体専用の鍵データとなる鍵データ又は固定値データのいずれかを用いて上記デコーダからの出力データに施されている暗号を解く解読処理部とを備えている記録媒体の再生装置。

【請求項 18】 上記解読処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータと上記記録媒体から読み出されたアプリケーション鍵データとを用いて上記デコーダの出力データからコンテンツ鍵データを取り出すディクリプタとを備えている請求項 17 に記載の記録媒体の再生装置。

【請求項 19】 上記解読処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータと上記記録媒体から読み出されたアプリケーション鍵データとを用いて演算処理を行い、上記演算処理の結果得られるデータを上記ディクリプタに暗号解読の鍵データとして供給する演算処理部を備えている請求項 18 に記載の記録媒体の再生装置。

【請求項 20】 上記装置は、更に上記演算処理部に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータを選択的に供給する選択処理部を備えている請求項 19 に記載の記録媒体の再生装置。

【請求項 21】 上記記録媒体には、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録されており、上記装置は更に上記デコーダの出力データから上記識別データを読み取る読み取り部を備え、上記読み取り部からの出力データにより上記選択処理部が制御される請求項 20 に記載の記録媒体の再生装置。

【請求項 22】 上記解読処理部は、更に上記デコーダの出力データに施されている暗号を上記コンテンツ鍵データを用いて解読する更なるディクリプタとを備えている請求項 18 に記載の記録媒体の再生装置。

【請求項 23】 コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化されて記録されているとともに、上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録された記録媒体から上記識別データを読み出し、上記読み出された識別データによって上記コンテンツデ

ータが上記固定値データによって暗号化処理されていると判別されたときには、上記記録媒体から読み出されたデータを上記固定値データによって暗号の解読処理を行い、

上記読み出された識別データによって上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データによって暗号化されていると判別されたときには、上記記録媒体から読み出されたコンテンツデータを上記記録媒体から読み出された上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いて暗号の解読処理を行う記録媒体の再生方法。

【請求項 24】 上記方法は、上記記録媒体が上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データで暗号化されて記録された記録媒体か、上記固定値データを用いて上記コンテンツデータが暗号化されて記録された記録媒体のいずれでもない場合には再生処理を中止する請求項 23 に記載の記録媒体の再生方法。

【請求項 25】 暗号化されたコンテンツデータが記録されるデータ領域と、

上記データ領域に先立って読み出される位置に設けられ、上記データ領域の管理データと、上記コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データとを含むデータが記録される管理データ領域とを備えている記録媒体。

【請求項 26】 上記管理データ領域には、上記固定値データが記録されている請求項 25 に記載の記録媒体。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正内容】

【0001】

【発明の属する技術分野】この発明は、暗号化によってセキュリティを保つようにしたデータを記録する記録媒体の記録装置および方法、記録媒体の再生装置および方法、並びに記録媒体に関する。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正内容】

【0006】したがって、この発明の目的は、メディアにバインドした鍵を使用して暗号化する本格的なセキュリティ機能の導入を容易とすることが可能な記録媒体の記録装置および方法、記録媒体の再生装置および方法、並びに記録媒体を提供することにある。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0007

【補正方法】変更

【補正内容】

【0007】

【課題を解決するための手段】上述した課題を達成するために、請求項 1 の発明は、入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理を施す暗号化処理部と、暗号化処理部からの出力データにエンコード処理を施すとともに、暗号化処理部で記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込むエンコード処理部と、エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録媒体の記録装置である。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正内容】

【0008】請求項 9 の発明は、入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、暗号化処理されたデータにエンコード処理を施す際に、暗号化処理の際に記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、エンコード処理されたデータを記録媒体に記録する記録媒体の記録装置である。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正内容】

【0009】請求項 17 の発明は、コンテンツデータが暗号化されて記録されている記録媒体からデータを読み出すヘッド部と、ヘッド部からの信号にデコード処理を施すデコーダと、記録媒体から読み出された記録媒体に記録されることによって記録媒体専用の鍵データとなる鍵データ又は固定値データのいずれかを用いてデコーダからの出力データに施されている暗号を解く解読処理部とを備えている記録媒体の再生装置である。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正内容】

【0010】コンテンツデータが記録されることによっ

て記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号されて記録されているとともに、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録された記録媒体から識別データを読み出し、読み出された識別データによってコンテンツデータが固定値データによって暗号化処理されていると判別されたときには、記録媒体から読み出されたデータを固定値データによって暗号の解読処理を行い、読み出された識別データによってコンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データによって暗号化されていると判別されたときには、記録

媒体から読み出されたコンテンツデータを記録媒体から読み出された記録されることによって記録媒体専用の鍵データとなる鍵データとを用いて暗号の解読処理を行う記録媒体の再生方法である。請求項 25 の発明は、暗号化されたコンテンツデータが記録されるデータ領域と、データ領域に先立って読み出される位置に設けられ、データ領域の管理データと、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データとを含むデータが記録される管理データ領域とを備えている記録媒体である。